# INTRODUCTION TO APPLIED CRYPTOGRAPHY

# Cryptography, old and new

- Crypto is an ancient discipline
- Recall:
  - Julius Caesar
  - Enigma machine
- Cryptography as a science (modern cryptography) has a short, but exciting history. Most of it has occurred within the last **40 years**

This course is an introduction to
**modern cryptography**

# Main Goals of Cryptography

- Data Privacy
- Data Authenticity
  - message came from where it claims
- Data Integrity
  - message has not been modified on the way

# When is Cryptography used?

- Online shopping and banking
- Using a cell phone
- Paying with credit cards
- …

*Half of the internet is now encrypted!*

# Players and Settings


1. Symmetric-key setting

# Players and Settings

| | |
|---|---|
| ... | ... |
| $\mathcal{R}$ | $pk_{\mathcal{R}}$ |
| ... | ... |


2. Asymmetric (public)-key setting

# Goals and Primitives (tools)

| goal \ setting | symmetric-key | asymmetric-key |
|---|---|---|
| data privacy | symmetric (secret-key) encryption | asymmetric (public-key) encryption |
| data authenticity/integrity | message authentication code (MAC) | digital signature scheme |

# Course Objectives

- We will study the practical solutions for the basic cryptographic goals in each setting, e.g.
  - AES-based modes of operation
  - HMAC
  - RSA-OAEP encryption
  - RSA and DSA signatures
  - …
- We will also learn the more fundamental principles of:
  - What is a good scheme
  - How to estimate and compare security

# How good is a Scheme?

- “Trial and error” approach

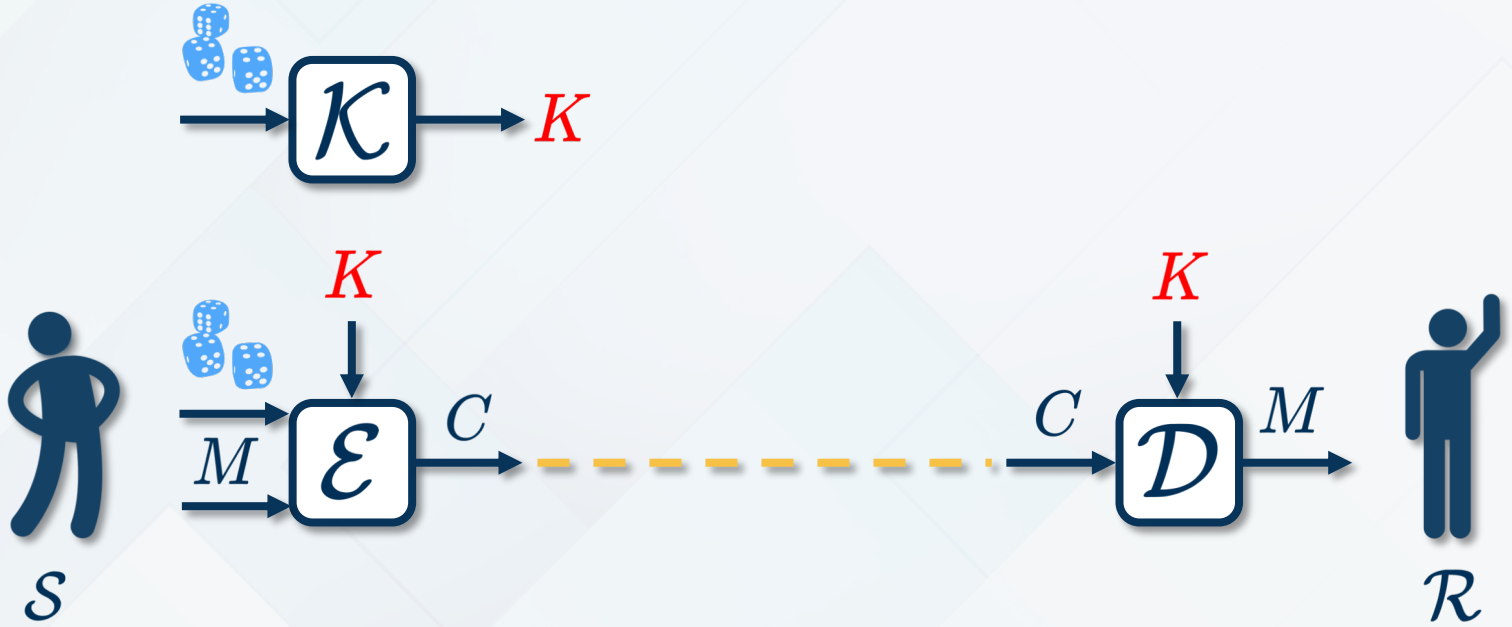
  1. Try to find an attack
  2. If an attack is found, the scheme is insecure.
  Fix the scheme and repeat step 1
  3. If no attack is found then…?

- “Provable security” approach
  - Show that if an attack is found (a scheme is insecure), then one can break some trusted assumptions (e.g. factoring)
  - Requires a definition of what “secure” means

# SYMMETRIC ENCRYPTION

# Syntax of Symmetric Encryption

- A symmetric encryption scheme consists of descriptions of …
  - The message space $\mathcal{MsgSp}$
  - The key generation algorithm $\mathcal{K}$ (or the key space $\mathcal{KeySp}$)
  - The encryption algorithm $\mathcal{E}$
  - The decryption algorithm $\mathcal{D}$




It is required that for every $M \in \mathcal{M}sg\mathcal{S}p$ and every $K \in \mathcal{K}ey\mathcal{S}p$ (or output by $\mathcal{K}$), $\mathcal{D}(K, \mathcal{E}(K, M)) = M$

# OneTimePad

- OneTimePad $= (\mathcal{K}, \mathcal{E}, \mathcal{D})$, $\mathcal{M}sg\mathcal{S}p = \{0,1\}^n$

  $\mathcal{K}$ return a random n-bit string $K$ $\mathcal{K}ey\mathcal{S}p = \{0,1\}^n$

  $\mathcal{E}(K, M) : C \leftarrow M \oplus K$ return $C$

  $\mathcal{D}(K, C) : M \leftarrow C \oplus K$ return $M$

- Example

  $M = 011111111011101$

  $K = 110010011010100$

  $C = 101101100001001$

# Intuition for Security

- Ciphertexts do not give the adversary ANY new information

# Perfect (Shannon) Security

- Def: an encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is Shannon-secure, if for every ciphertext $C$ and messages $M_1, M_2$

$$\Pr[\mathcal{E}(K, M_1) = C] = \Pr[\mathcal{E}(K, M_2) = C]$$

## Theorem

- OneTimePad is a perfect-secure encryption scheme

## Proof

- Fix any ciphertext $C \in \{0,1\}^n$
- For every M, $\Pr[\mathcal{E}(K, M) = C] = \Pr[K = M \oplus C] = 2^{-n}$

# Theorem (*Shannon's theorem, optimality of OneTimePad)*

- If a scheme is Shannon-secure, then $|\mathcal{K}ey\mathcal{S}p|$ cannot be smaller than $|\mathcal{M}sg\mathcal{S}p|$

## Proof

- Fix a ciphertext $C$ (by picking $M_1, K$ and setting $C = \mathcal{E}(K, M_1)$

  Thus $\Pr[\mathcal{E}(K, M_1) = C] > 0$
  - Assume there exists $M_2$ such that $\Pr[\mathcal{D}(K, C) = M_2] = 0$
  - By the correctness requirement $\Pr[\mathcal{E}(K, M_2) = C] = 0$
  - Therefore $\Pr[\mathcal{E}(K, M_1) = C] \neq \Pr[\mathcal{E}(K, M_2) = C]$ that violates Shannon secrecy
  - Thus for every $M_2 \in \mathcal{M}sg\mathcal{S}p$ there exists $K' \in \mathcal{K}ey\mathcal{S}p$
  - $\mathcal{D}(K', C) = M_2$ and $|\mathcal{K}ey\mathcal{S}p| \geq |\mathcal{M}sg\mathcal{S}p|$

- So we cannot do better than the OneTimePad, but we know it is impractical (why?). Is it the end?

  **YES**, of the “information-theoretic” crypto

  **NO**, if we relax the security requirement, and assume that adversaries are computationally bounded

- We will also assume that…
  - There are some ”hard” problems
  - Secret keys are kept secret
  - Algorithms are public (Kerckhoff’s principle)

We move to the area of “**computational-complexity**” crypto, that opens many possibilities